UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,065	02/03/2004	W. Dale Hopkins	200309349-1	4532

22879 7590 04/10/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

NOTIFICATION DATE	DELIVERY MODE
04/10/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/772,065	HOPKINS, W. DALE	
	Examiner	Art Unit	
	MICHAEL J. SIMITOSKI	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) *18* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *7,13-17,19-23 and 25-30* is/are rejected.

7)☒ Claim(s) *1-6,8-12 and 24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/3/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The IDS of 2/3/2004 was received and considered.

2. Claims 1-30 are pending.

Election/Restrictions

3. Applicant's election of species I in the reply filed on 12/4/2007 is acknowledged. Because applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (MPEP § 818.03(a)). Claim 18 is withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected specie, there being no allowable generic or linking claim. Based on the potential allowable subject matter described below, claims 9-11 & 26 are rejoined.

Claim Objections

4. Claims 1-12 & 23-27 are objected to because of the following informalities:

   a. Regarding claim 1 (and 2-12 by dependence), the limitation "the secret unique key" (line 6) should be replaced with "the unique key".

   b. Regarding claim 23 (and 24-27 by dependence), the limitation "and transaction sequence number" (last two lines) should be replaced with "and a transaction sequence number".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 7, 13-17, 19, 20-23 & 25-30 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

c. Regarding claim 7, the limitation "the cryptogram C" (line 3) lacks sufficient antecedent basis.

d. Regarding claim 13, the limitations "capable of" (lines 2, 4) are unclear because a capability is claimed rather than apparatus limitations required to achieve the capability. Therefore, the scope of these limitations is unclear. The limitations following "capable of" are not considered.

e. Regarding claim 13, the limitation "the point of entry" (last line) lacks sufficient antecedent basis.

f. Regarding claim 20, the limitations "capable of" (lines 2, 5 & 9) are unclear because a capability is claimed rather than apparatus limitations required to achieve the capability. Therefore, the scope of these limitations is unclear. The limitations following "capable of" are not given

patentable weight. For the limitation in line 9, it is understood that program code can impart functionality on a processor when executed. This limitation is read "program code embodied therein causing the processor ...".

g. Regarding claim 21, the limitation "capable of" (line 3) is unclear because a capability is claimed, raising the question as to whether the code actually performs the steps. Therefore, the scope of these limitations is unclear. However, it is understood that program code can impart functionality on a processor when executed. This limitation is read "program code causing the processor ...".

h. Regarding claim 22, the limitation "capable of" (lines 3, 8, 11 & 17) is unclear because a capability is claimed, raising the question as to whether the code actually performs the steps. Therefore, the scope of these limitations is unclear. However, it is understood that program code can impart functionality on a processor when executed. This limitation is read "program code causing the processor ...".

i. Regarding claim 23, the limitations "capable of" (lines 2, 5 & 8) are unclear because a capability is claimed rather than apparatus limitations required to achieve the capability. Therefore, the scope of these limitations is unclear. The limitations following "capable of" are not given patentable weight. For the limitation in line 8, it is understood that

program code can impart functionality on a processor when executed. This limitation is read "program code embodied therein causing the processor ...".

j. Regarding claim 25, the limitation "capable of" (lines 3, 5, 7, 14, 19 & 24) is unclear because a capability is claimed, raising the question as to whether the code actually performs the steps. Therefore, the scope of these limitations is unclear. However, it is understood that program code can impart functionality on a processor when executed. This limitation is read "program code causing the processor ...".

k. Regarding claim 26, the limitation "capable of" (lines 3, 5, 7, 12 & 17) is unclear because a capability is claimed, raising the question as to whether the code actually performs the steps. Therefore, the scope of these limitations is unclear. However, it is understood that program code can impart functionality on a processor when executed. This limitation is read "program code causing the processor ...".

l. Regarding claim 27, the limitation "capable of" (line 3) is unclear because a capability is claimed, raising the question as to whether the code actually performs the steps. Therefore, the scope of these limitations is unclear. However, it is understood that program code can impart functionality on a processor when executed. This limitation is read "program code causing the processor ...".

m. Regarding claim 28, the limitation "capable of" (line 9) is unclear because a capability is claimed rather than apparatus limitations required to achieve the capability. Therefore, the scope of these limitations is unclear. For the purposes of this action, in light of the rest of the claim, the limitation "being capable of" is understood to be removed.

n. Regarding claim 29, the limitation "capable of" (line 9) is unclear because a capability is claimed rather than apparatus limitations required to achieve the capability. Therefore, the scope of these limitations is unclear. For the purposes of this action, in light of the rest of the claim, the limitation "being capable of" is understood to be removed.

o. Regarding claim 30, the limitation "capable of" (line 9) is unclear because a capability is claimed rather than apparatus limitations required to achieve the capability. Therefore, the scope of these limitations is unclear. For the purposes of this action, in light of the rest of the claim, the limitation "being capable of" is understood to be removed.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claim 20-22 are rejected under 35 U.S.C. 102(b) as being anticipated by "Efficient Identification and Signature Schemes" by **Ohta**.

Regarding claim 20, Ohta discloses an apparatus comprising an enrollment system (centre issuing smart cards, ¶1 & ¶4) comprising a communication interface (inherent as the smart card computes receives values, ¶5) capable of communicating with a writer configured to accept a smart card (values are written to card, ¶5), a processor coupled to the communication interface (inherent as S_i is computed, ¶5) and a memory coupled to the processor and having a computable readable program code (algorithm) embodied therein capable of causing the processor to initialize and personalize a smart card with a unique key per smart card (S_i is computed and recorded on the smart card, ¶5), the unique key derived from a private key (d) that is assigned an distinctive to systems and a card base of a card issuer (centre, ¶4).

Regarding claim 21, Ohta discloses a computable readable program code capable of causing the processor to write to an enrolled smart card a stored public entity-identifier (I_i is stored because the card sends it to the verifier, ¶6 Step 1) and the secret unique key (S_i, ¶5).

Regarding claim 22, Ohta discloses a computable readable program code capable of causing the processor to define public key values (e, N) that

are exclusive to a card issuer system and card base (¶5), the key value e being a public exponent (¶4) and a key value N (n) is a modulus in an RSA system (¶¶2-4), a computable readable program code capable of causing the processor to define a private key value d (¶¶4-5) that is exclusive to a card issuer system and card based, the private key value d being a secret RSA private key (¶5), a computable readable program code capable of causing the processor to compute a secret key u (S_i, ¶5) that is unique to the smart card using an equation of the form u=x^d(mod N) ($S_i = I_i^d \bmod n$, ¶5), where x (I_i) is an entity-identifier that identifies the smart card and the entity (user, ¶4) and a computable readable program code capable of causing the processor to store the secret key u (S_i, ¶5) on the smart card with the public key values x, e and N (I_i, e, n, ¶5).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ohta** in view of U.S. Patent 4,288,659 to **Atalla**.

Regarding claim 13, Ohta discloses a smart card (p. 115, ¶5) comprising an interface capable of communicating with a card reader and/or writer (inherent as the card is written with S_i, ¶5), a processor coupled to the interface (microprocessor, ¶1) and a memory coupled to the processor (¶14) that stores a public entity-identifier (n, e, ¶5) and a secret unique key (S_i, ¶5) derived from a private key (d) that is assigned and distinctive to systems and a card base of a card issuer ($S_i = I_i^d \bmod n$, ¶5), and a computable readable program code embodied therein (algorithm, inherent if RSA is performed, ¶15) that creates a PIN encryption key ($Y = S_i R^v \bmod n$, ¶6 Step 3) derived from the smart card unique key (S_i), but lacks creating a transaction identifier that uniquely identifies the point of entry and transaction sequence number. However, Atalla teaches that during a monetary transaction, a pair of input signals is encrypted, where the PIN from the authorized individual, a sequence number and a machine identification number (col. 2, lines 48-63) to identify the terminal and to create a unique transaction value (col. 2, lines 55-63). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ohta to create a sequence number and machine identifier and send this in the transaction. One of ordinary skill in the art would have been motivated to perform such a modification to identify the terminal/reader and to create a unique transaction value, as taught by Atalla.

Regarding claim 14, Ohta discloses a secret unique key u (S_i, ¶5) stored in memory (¶5) with public key values x, e and N (I_i, e, n, ¶5 and I_i is stored because the card sends it to the verifier, Step 1), wherein x (I_i) is an entity-identifier that identifies the smart card and the entity (¶4), a key value e is a public exponent (¶4) and a key value N (n) is a modulus in an RSA system (¶¶2-4), the public key values (e, N) being exclusive to a card issuer system and card base (¶5), wherein the secret key u is unique to the smart card and computed using an equation of the form u=x^d(mod N) ($S_i = I_i^d \bmod n$, ¶5), wherein the private key d is exclusive to the card issuer (private key, ¶5) and card based, the private key value d being a secret RSA private key (¶5).

11. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Ohta** & **Atalla**, as applied to claim 13 above, in further view of U.S. Patent 6,990,471 to **Rajaram**.

Regarding claim 19, Ohta lacks computing a hash. However, Rajaram teaches that a consumer with a smart card (Fig. 1, #114) uses the device to create a hash of receipt data to confirm a transaction (col. 5, lines 41-62). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ohta to include in the memory a computable readable program code capable of causing the processor to hash

transaction data elements and communicate the hash point-to-point to a card issuer (financial institution). One of ordinary skill in the art would have been motivated to perform such a modification to confirm a transaction's validity, as taught by Rajaram.

Potential Allowable Subject Matter

12. Claims 1-12 & 23-30, as best understood are believed to be allowable if any of the above rejections under 35 U.S.C. §112 and objections to the claims are overcome.

13. Claims 15-17 are objected to as being dependent upon a rejected base claim, but are believed to be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and any of the above rejections under 35 U.S.C. §112 and objections to the claims are overcome.

14. The following is a statement of reasons for the indication of allowable subject matter:

p. Regarding claim 1 (and claims 2-12 by dependence), **Ohta** discloses enrolling a smart card with a unique key per smart card, the unique key derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, an enrolled smart card containing a stored public entity-identifier and the secret unique key (see

above discussion with respect to claims 13 and 20). **Atalla** discloses the well known concept of transacting at a point of entry to a network where the transaction uniquely identifies the point of entry and a sequence number (see above discussion). However, the prior art of record fails to teach or disclose, either alone or in combination, communicating the PIN encryption key point-to-point in encrypted form through a plurality of nodes in the network and recovering the PIN at a card issuer server from the PIN encryption key using the card issuer private key, in combination with the other elements of the claims.

q. Regarding claim 15 (and claims 16-17 by dependence), the prior art of record fails to teach or disclose, either alone or in combination, computing an equation of the form $K = u \cdot TSN^{H} (\mathrm{mod}\, N)$, where K is a keying code, u is a secret key, TSN is a transaction sequence identifier that identifies the terminal and a sequence number for a transaction originating at the terminal, H is a hash of transaction data elements, in combination with the other elements of the claims.

r. Regarding claim 23 (and claims 24-27 by dependence), **Ohta** and **Atalla** are discussed above. However, the prior art of record fails to teach or disclose, either alone or in combination, causing the processor to recover a Personal Identification Number (PIN) from a transaction PIN encryption key received via the network using a card issuer private key,

the transaction PIN encryption key being derived from a smart card unique key initialized and personalized to the smart card and derived from the card issuer private key, and a transaction identifier that uniquely identifies the point of entry and transaction sequence number, in combination with the other elements of the claims.

s. Regarding claim 28, **Ohta** and **Atalla** are discussed above. However, the prior art of record fails to teach or disclose, either alone or in combination, creating, communicating, and decrypting a PIN encryption key derived from a smart card unique key and a transaction identifier that uniquely identifies a point of entry terminal and transaction sequence number, the smart card unique key being derived from a private key that is assigned and distinctive to systems and a card base of a card issuer, in combination with the other elements of the claim.

t. Regarding claim 29, **Ohta** and **Atalla** are discussed above. However, the prior art of record fails to teach or disclose, either alone or in combination, decrypting a PIN encryption key derived from a smart card unique key and a hash of transaction data elements, enabling simultaneous key management and integrity checking, in combination with the other elements of the claim.

u. Regarding claim 30, **Ohta** and **Atalla** are discussed above. However, the prior art of record fails to teach or disclose, either alone or in

combination, means for recovering the PIN at a card issuer server from the PIN encryption key using the card issuer private key, in combination with the other elements of the claim.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

v. The Chang reference is cited for teaching IBE, specifically creating a secret key (customized) using a card issuer's private key and an identity of the user, and computing a signature using a hash function (p. 1).

w. U.S. Patent 7,240,034 is cited for teaching the use of electronic wallets (smart cards) in transactions at points of entry and using a terminal ID and an anti-replace data in a transaction.

x. U.S. Patent 5,694,471 is cited for teaching storing ID data and a public key on a smart card.

y. U.S. Patent 6,105,008 is cited for teaching communicating a financial transaction over the Internet between a smart card and bank (over a indeterminate number of nodes, Fig. 4).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone